2020

Will Russia Influence the American Vote?

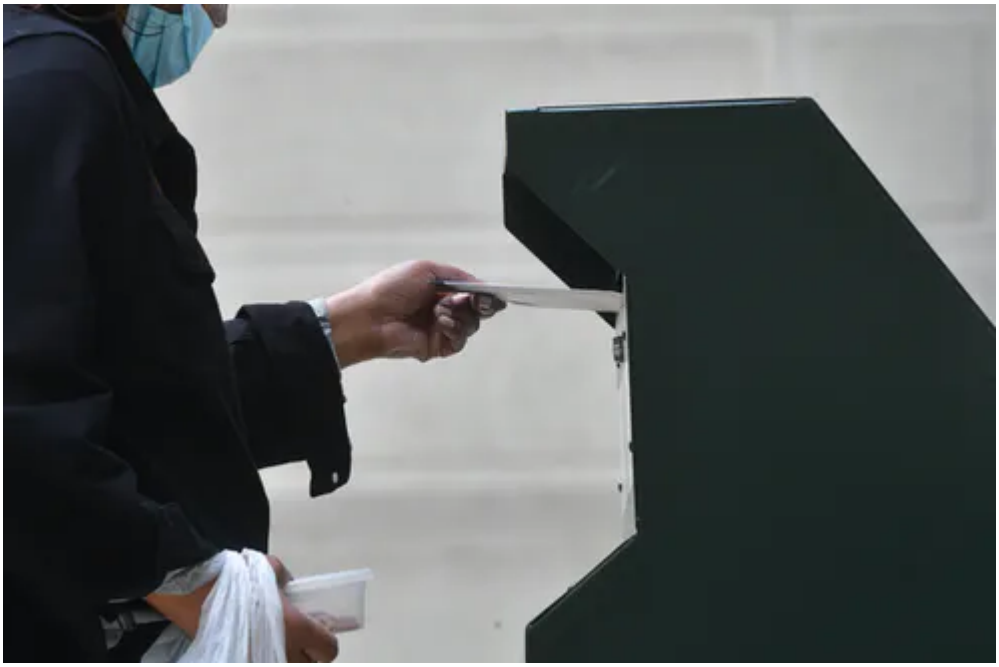
Jasper, Scott

Scott Jasper, Will Russia Influence the American Vote? The Conversation [Blog], October 29, 2020
http://hdl.handle.net/10945/65925

Close

THE CONVERSATION

Academic rigor, journalistic flair



As American voters cast their ballots, they are also being targeted with foreign disinformation. Mark Makela/Getty Images

Will Russia influence the American vote?

October 29, 2020 8.31am EDT

Author

Scott Jasper

Lecturer in National Security Affairs, Naval Postgraduate School

The idea that someone recently tried to influence Americans to vote for a particular candidate by sending them threatening emails may sound outlandish – as might federal officials' allegation that the Iranian government is behind those messages.

But U.S. voters should prepare for even more strange and unexpected examples of information warfare that manipulate, distort or destroy election-related information between now and Election Day – and perhaps beyond that, depending on whether there are questions about who may have won the presidency.

Since 2016, Americans have learned that foreign interests attempt to affect the outcomes of presidential elections, including with social media postings and television ads.

As a scholar of Russian cyber operations, I know other nations, and Russia in particular, will go to extreme measures to influence people and destabilize democracy in the U.S. and elsewhere.

Be on guard

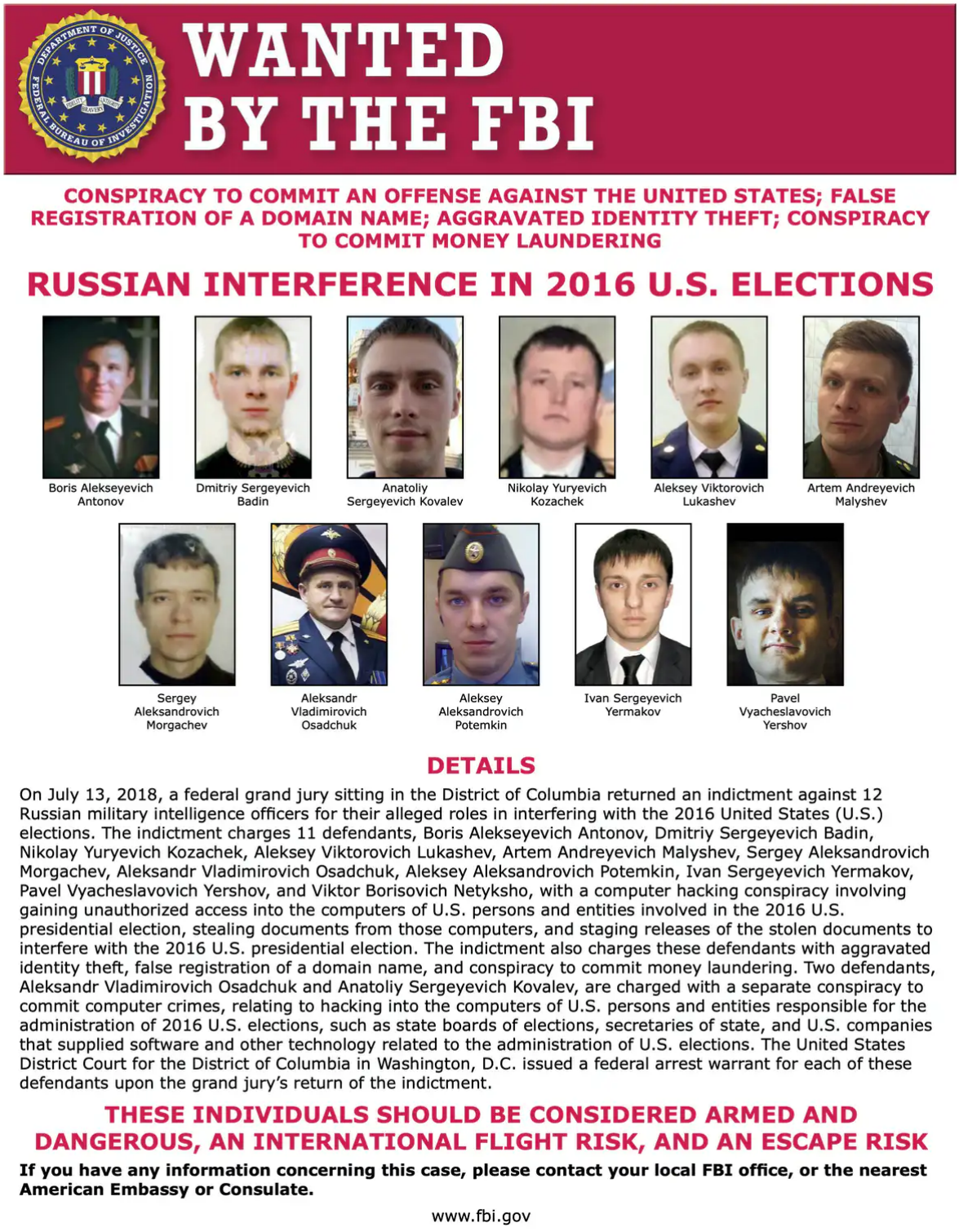
Here is what to look out for.

Other measures the Russians could still take include announcements aimed at influencing the vote, such as leaked emails and documents that may not be authentic.

Also, watch for claims that hackers have gained access to, or manipulated, state or local election systems. It doesn't have to be true for people to become worried, uncertain and untrusting of election results.

Be prepared to see ransomware attacks – software that seizes control of key computers and demands a ransom to unlock the system – on precincts in key battleground states, which may not aim to alter the vote, but rather stall the vote count and certification. A mid-October ransomware attack on Hall County, Georgia, government networks interrupted phone service and some computer systems, including a database used to verify voters' signatures.

Anything can happen – but Americans can be ready to skeptically and critically examine any announcements of attempted, or claims of successful, election interference.



Russian government agents interfered with the 2016 U.S. presidential election, and are poised to do so again. FBI

Misleading propaganda

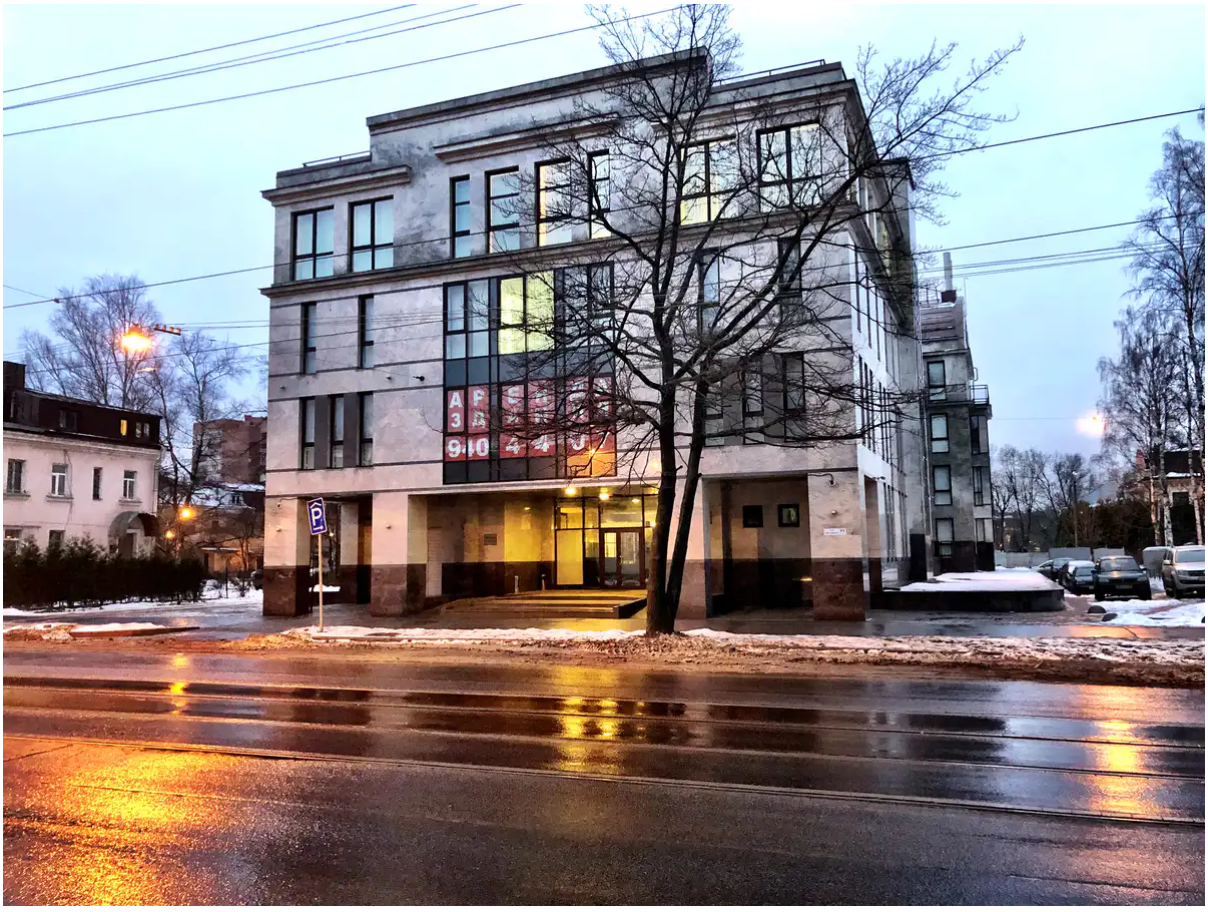
The real goal of information warriors – no matter where they are from, even beyond Russia and Iran – is to make it hard for Americans to know what is real.

In 2016, for instance, Russian disinformation operations created fake social media accounts claiming to be U.S. citizens, in hopes of spreading political division and conflict. They portrayed Hillary Clinton as weak and corrupt, which damaged her support among voters.

In this election cycle, the information warfare is more sophisticated. Russian-made propaganda has portrayed Joe Biden as incompetent and corrupt – but has also claimed that U.S. democracy is failing. Examples include an episode on a Kremlin-controlled Sputnik show titled "How much money to buy the presidency? Bloomberg tries to find out" and an episode called "Iowa Caucus Chaos: People are Losing Confidence in Election Results" on its sibling Russia Today video network. These outlets are available across the U.S. on radio, cable and satellite TV systems, and online – including on conservative websites.

Russian information warriors are impersonating real advocacy groups. They even created a now-defunct news website named Peace Data, which used fake names and photos for its editors, but hired unsuspecting real journalists as freelancers and ordered them to write stories critical of Biden, discussing corruption, abuse of power and human rights violations.

Some of the stories were also hostile to Trump, which indicates that the main goal remains to sow division in the United States.



A building in St. Petersburg, Russia, where U.S. officials allege Russian trolls worked to interfere with the 2016 U.S. presidential election. Voice of America via Wikimedia Commons

Visible responses

Fortunately, businesses, federal cybersecurity officials and intelligence leaders are signaling that they are more willing than they were in 2016 to sound the alarm about foreign interference in the U.S. presidential election.

For instance, in August, the National Security Agency warned the cybsersecurity community about malicious software written by the Russian military, including details of the military unit involved, as well as advice on how system administrators can protect their networks and servers.

And in September, Microsoft reported that a Russian hacking group has attempted to intrude into the digital files of at least 200 organizations tied to the 2020 U.S. election. It targeted political campaigns, advocacy groups, parties and political consultants. Affiliated with Russian military intelligence, this is the same group that hacked and leaked damaging Democratic Party emails in 2016.

In late October, Director of National Intelligence John Ratcliffe and FBI Director Christopher Wray alleged that Russia and Iran had obtained U.S. voter registration information, at least some of which is publicly available. They also claimed – without offering evidence – that Iran is responsible for sending threatening emails to voters in as many as four states, including Florida and Alaska, that reportedly said "You will vote for Trump on Election Day or we will come after you."

Big technology platforms have also taken steps to fight disinformation. Facebook took down a network of fake accounts linked to Russian military intelligence. Facebook will not post political ads in the week week before Election Day and Google will reject all election-related ads after Election Day to prevent false claims.

Twitter has also shut down accounts that it could reliably attribute to Russian-sponsored entities. And Twitter has sought to slow the spread of posts by limiting retweeting – though that has concerned Republicans, who fear this measure will stifle conservatives' speech.

Director of National Intelligence Announcess That They have Identified Russia And Iran As Actively Meddling In The U.S. Election

U.S. officials make a presentation about foreign information warfare.

Post-vote chaos

The week after Election Day could be volatile, especially if mail-in ballots are slow to be counted and results appear to change as the count continues.

Russia could use social media accounts that have not yet been detected to push reports of voter suppression or ballot fraud, trying to convince the public that election results are somehow inaccurate. U.S. Cyber Command might take Russian troll servers offline, as it did during the 2018 U.S. midterm election.

Meanwhile, voters can protect themselves by being skeptical of urgent or alarming claims in online media, and by remembering that they may be targets of disinformation campaigns. U.S. security agency efforts might stop Russia from altering the vote count, but sowing discord about its integrity could be enough to serve Russia's goal of undermining democracy.

[*Expertise in your inbox. Sign up for The Conversation's newsletter and get expert takes on today's news, every day.*]

Propaganda **Information warfare** **Misinformation** **Disinformation** **Russian propaganda** **2020 US elections** **Russian information warfare**